AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph starting at page 14, line 2 with the following amended paragraph:

A private information protection method according to a first embodiment of the present invention is described while referencing FIG. 1, FIG. 2, and FIG. 3. "En(X)" in FIG. 1 denotes information generated by encrypting data X using an encryption key and can be decrypted by an n-th server. "E3(DATA1)", for example, denotes information generated by encrypting DATA1 using an encryption key and can be decrypted by a ~~second~~ third server 74. In FIG. 1, a case with n = 3 is exemplified.

Please replace the paragraph starting at page 14, line 10 with the following amended paragraph:

First, a ubiquitous computing system shown in FIG. 1 includes a portable information terminal 10a, which plays a role as a first wearable computer that a user utilizes, a meta server 76, which is made up with a plurality of servers processing transmission source metadata MD0 transmitted from the first wearable computer (portable information terminal) 10a, and a transmission destination server R40. The meta server 76 is assumed to include a group of servers such as a first server 72, a second server 73, a ~~second~~ third server 74, and a transmission server 24, a first anonymous communication path 71a, a second anonymous communication path 71b, and a third anonymous communication path 71c, which connect between respective servers, and an encrypted information database 25 connected to the second server 73. In reality, there is no limitation on the number of servers, the number of transmission paths, and the number of databases. "Anonymous communication path" denotes a communication path that prevents transmitted packet information from being read by third parties, and may be a LAN cable connection communication path, a wireless connection communication path, or a dedicated line connection communication path.

Please replace the paragraph starting at page 15, line 6 with the following amended paragraph:

(a) The first wearable computer (portable information terminal)10a generates a first encrypted information E1 (DATA3) by encrypting first information data DATA3 using an encryption key that allows only the first server 72 to decrypt, generates a second encrypted information E2 (DATA2) by encrypting second information data DATA2 using an encryption key that allows only the second server 73 to decrypt, and generates a third encrypted information E3 (DATA1) by encrypting third information data DATA1 using an encryption key that allows only the ~~second~~ third server 74 to decrypt while the meta server 76 receives transmission source metadata MD0. The DATA1, DATA2, DATA3, ... may be information such as private authentication information, terminal information, transmission destination information, merchandise information, mail information, or image information.

Please replace the paragraph starting at page 16, line 6 with the following amended paragraph:

(c) The second server 73 having received the first transmission metadata MD1 detects decryptable information necessary for the second server 73 to process it. Since there is E2(DATA2) shown in FIG. 1, it is then decrypted using the same method as that used by the first server 72, providing the DATA2, which is then processed (not shown in the drawing). Afterwards, the DATA2 is encrypted again and replaced with the resulting ER(DATA2), allowing the transmission destination server R40 to decrypt it. The second server 73 also conducts processing such as adding information using information that cannot be decrypted to know the content thereof. In FIG. 1, E3(DATA1) is decrypted by the ~~second~~ third server 74, and the n+1-th encrypted information E3(INFO2) is then retrieved from the encrypted information database 25, which is connected to the second server 73, using this E3(DATA1) as key information. The resulting E3(INFO2) is then added forming a second transmission metadata MD2, which is then transmitted to the ~~second~~ third server 74 via the second anonymous communication path 71b.

Please replace the paragraph starting at page 16, line 22 with the following amended paragraph:

(d) The ~~second~~ third server 74 having received the second transmission metadata MD2 detects decryptable information necessary for the ~~second~~ third server 74 to process. In FIG. 1, since there are E3(DATA1) and E3(INFO2), these are then decrypted, using the same method as that used by the first server 72, to DATA1 and INFO2, which are then processed. Afterwards, the DATA1 and INFO2 are encrypted again and replaced with the ER(DATA1) and the ER(INFO2), allowing the transmission destination server R40 to encrypt them. The third transmission metadata MD3 is generated and transferred to a transmission server 24 via the third anonymous communication path 71c.

Please replace the paragraph starting at page 17, line 7 with the following amended paragraph:

(e) The transmission server 24 transmits the third transmission metadata MD3 to the transmission destination server R40 outside of the meta server 76 in conformity with a transmission address. The information in the final third transmission metadata MD3 has gone through and been encrypted by the first server 72, the second server 73, and the ~~second~~ third server 74 so that it can be decrypted by the transmission destination server R40.

Please replace the paragraph starting at page 27, line 13 with the following amended paragraph:

As shown in FIG. 10, an encryption key acquisition system according to a sixth embodiment of the present invention is organized by a first wearable computer (portable information terminal) 10a used by a user, a first server 72 configured to process transmission source metadata MD0 transmitted from the first wearable computer 10a, and an encrypted information database 25a connected to the first server 72. However, the first server 72 is described as an arbitrary server in the meta server made up of a plurality of servers. Here, "E1(DATA2)" shown in FIG. 8 is described as service information. The service information includes information necessary for merchandise or service transactions, and may be merchandise information such as size and color, business information, or delivery information.

Please replace the paragraph starting at page 36, line 3 with the following amended paragraph:

(c) When the authentication image is presented by the first communication terminal 20a in step S204, the second communication terminal (authentication terminal) 20b photographs the presented authentication image and then stores it in the image data storage unit 12b in step S205. Furthermore, in step S206, the second communication terminal (authentication terminal) 20b generates authentication information by combining the information of the authentication image stored in the image data storage unit 12b and the authentication identifier of the second communication terminal (authentication terminal) 20b stored in the authentication information storage unit 302a, and in step S207, the authentication information is then transmitted to the information-processing server 300~~07~~.

Please replace the paragraph starting at page 40, line 17 with the following amended paragraph:

(c) Processing of steps S354 through ~~S260~~ S360 thereafter is the same as that of the steps S202 through S208 in FIG. 13 and description thereof is thus omitted.

Please replace the paragraph starting at page 90, line 24 with the following amended paragraph:

(c) The information-processing server 30 confirms that the action is authorized for the second portable information terminal 20t, and prepares specific information of the first portable information terminal 20s using the structural information of the second portable information terminal 20t. In step S922, the specific information obtained from the first portable information terminal ~~20p~~ 20s is then transmitted to the second portable information terminal 20t in a form in conformity with the structure thereof.